IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:		)
		) ATTORNEY FILE NO.: SLA1055
Inventors:	Sridhar Dathathraya	)
		)
Serial No.:	09/944,695	)
		) Examiner: Ha, Leynna
		)
Filed:	August 31, 2001	) Customer No.: 55,286
		)
Title:	SYSTEM AND METHOD FOR SECURE COMMUNICATIONS WITH NETWORK PRINTERS	) Group Art: 2135
		)
		) Confirmation No.: 2135
		)

Board of Patent Appeals and Interferences
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF ON APPEAL

This is an appeal from the rejection by Examiner Leynna Ha, Group Art Unit 2135, of claims 1-8, 10-25, and 27-35 as set forth in the CLAIMS APPENDIX, all claims in the application.

REAL PARTY IN INTEREST

The real party in interest is Sharp Laboratories of America, Inc., as assignee of the present application by an Assignment in the United States Patent Office with a Recordation Date of August 31, 2001, at Reel 012147, Frame 0316.

RELATED APPEALS AND INTERFERENCES

None.

STATUS OF THE CLAIMS

Claims 1-8, 10-25, and 27-35 are in the application.

Claims 1-8, 10-25, and 27-35 are rejected.

Claims 1-8, 10-25, and 27-35 are appealed.

STATUS OF AMENDMENTS

In response to the Final Office Action of June 27, 2005, an amendment was filed, which attempted to add a new claim and to enter into the record the affidavit of Joey Lum. As noted in the Advisory Action mailed on September 13, 2205, the new claim and affidavit have not been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

The invention of claims 1 and 12 describes a simple method for secure communications to a network-connected printer. As shown in Fig. 5 (see Evidence Appendix, Attachment B) and described in the specification at page 10, ln. 6 through page 11, ln. 25 (see Evidence Appendix, Attachment A), the present invention method initially encrypts a document (i.e., at a personal computer) using a public key algorithm. As is well known in the art, the public key system uses a pair of asymmetric keys to encrypt and decrypt a document. The document is initially encrypted using a public key, associated with an individual (i.e., Bob). The public key can be downloaded by anyone in the general public (i.e., from a publicly accessible website). However, the document can only be decrypted using a corresponding private key, which Bob keeps secret. That is, only Bob can decrypt the document, because only Bob holds the private key.

As a second step in the method, the printer accepts a private key. Then, the printer downloads the encrypted document from a network server. Finally, the printer uses the private key to decrypt the downloaded document. The novelty of the invention stems from the fact that a printer cannot begin printing a document until the user shows up at the printer and supplies their private key. Thus, the user need not sprint to the printer after they press the "print" button on their PC, or worry that their printed personal document will sit in the document tray of an unintended destination printer, for anyone to read. As explained in more detail below, the prior art security schemes necessarily operate in a different mode because they are protecting a different entity than person printing the document.

The invention is also recited from the perspective of a system of networked devices (claim 19) and a network-connected printer (claim 29). Details of these claims are presented in the specification at page 5, ln. 8 through page 7, ln. 10, in the description of Figs. 3 and 4. Generally, the operation of the devices of claims 19 and 29 resembles the methods of claims 1 and 12, described above.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Whether claims 1-8, 10-25, and 27-35 are unpatentable under 35 U.S.C. 103(a) with respect to Mazzagatte et al. ("Mazzagatte"; US Patent 6,862,583), in view of DeBry (US Patent 6,385,728.

ARGUMENT

1. The rejection of claims 1-8, 10-25, and 27-35 under 35 U.S.C. 103(a) as unpatentable with respect to Mazzagatte et al. ("Mazzagatte"; US Patent 6,862,583), in view of DeBry (US Patent 6,385,728.

With respect to claims 1, 12, 19, and 29, the Final Office Action states that Mazzagatte describes the claim elements of encrypting documents with a public key, spooling encrypted documents to a server, notifying the printer of spooled documents, accepting a private key at the printer, decrypting the documents using a private key, and printing. The Office Action acknowledges that Mazzagatte does not describe any public key encryption details, but states that DeBry describes using a symmetric key to encrypt documents, and encrypting the symmetric key with a public key. The Office Action states that it would have been obvious to combine Mazzagatte with DeBry because encrypting the document with a public key prior to transmission, where the private key is used for decryption, would prevent unauthorized printing and spoofing.

An invention is unpatentable if the differences between it and the prior art would have been obvious at the time of the invention. As stated in MPEP § 2143, there are three requirements to establish a *prima facie* case of obviousness.

> First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck* 947 F.2d 488, 20 USPQ2d, 1438 (Fed. Cir. 1991).

Generally, Mazzagatte describes a process that transmits an unencrypted document using a secure protocol, such as SSL, to a printer, along with a form of identification (Fig. 5). At the printer, the document is encrypted and stored. Figs. 6, 7A, and 7B describe the operations performed at a printer. To print a document, the user presents identification to the printer. Then, the printer decrypts the document and prints it. As acknowledged in the Office Action, Mazzagatte does not discuss using a public key to encrypt the print job.

DeBry's encryption process is summarized in col. 11, lines 1-15. DeBry initially encrypts a document, at the source, using a symmetric key. Then, the symmetric key is encrypted using the printer's public key. The Applicant notes that a symmetric key is not a public or private key, but rather, a secret key. The encrypted document and encrypted symmetric key are stored on a print server. At print time, the printer accepts the encrypted document and the encrypted symmetric key from the server. The printer uses its private key to decrypt the encrypted symmetric key. Then, it uses the recovered symmetric key to decrypt the document.

Generally, DeBry describes a conventional digital envelope process. DeBry encrypts the document using a symmetric key, which is generally understood to be a randomly generated, secret key. When the randomly generated symmetric key is encrypted using a public key, a "digital envelope" is created. The symmetric key-encrypted document and digital envelope are transmitted together. The recipient's private key is used to recover the symmetric key from the digital envelope. Then, the document can be decrypted using the symmetric key.

With respect to the first *prima facie* requirement, the motivation to combine prior art references cannot be based upon a desired result of preventing "unauthorized printing and spoofing", as suggested in the Office Action. Rather, the motivation must come from a process detail of the DeBry system that can be applied to the Mazzagatte system. Further, even if an actual motive for combining references can be found, the combination of references must suggest a modification to one of the references that makes the claimed invention obvious.

In fact, the combination of references suggests an invention that, unlike the claimed invention, can be spoofed. As noted above, Mazzagatte's system only encrypts a document at the destination printer. Mazzagatte's system provides very limited safeguards. In DeBry's system a spoofer can intercept documents if they are able to fake the certification of a system printer. Once the system accepts the public/private key of a spoofer as legitimate, the spoofer can intercept documents. The source encrypts its symmetric key using a public key that has been "verified". The flaw in the system is that the source sends its symmetric key along with the document. If the symmetric key has been encrypted using a spoofer's public key, the spoofer is able to easily decrypt the symmetric key and gain access to the document.

The issue of motivation does not concern itself with whether there is some element of commonality between references. If it did, then any two references could be combined merely as the result of a common keyword. Although a prior art device "may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion of motivation in the references to do so." *In re Mills*, 916 F.2d 680, 682, 16 USPQ2d 1430, 1432 (Fed. Cir. 1990). Here, the analysis must determine if there is any motivation to modify either Mazzagatte or DeBry in such a manner as to teach the claimed invention. DeBry may provide a motivation to modify Mazzagatte, to perform some kind of encryption process. However, it is not the claimed invention process.

The proof of this statement can be seen in the operation of the claimed invention. In the claimed invention, the document is encrypted using a key pair where the user controls the private key. That is, the document is not encrypted using someone else's public key (associated a private key beyond the control of the user). Further, in the claimed invention, even if the document is misdirected or stolen in route to the printer, the document cannot be decrypted. In fact, even if the document is sent to the correct printer, the document cannot be stolen by someone who "runs to the printer" before the user, because the decryption cannot be enabled until the user arrives at the printer and enters their private key. Even if the prior art references are combined, they do not suggest the use of a private key as recited in the claimed invention, which prevents a document from printing until the user presents the private key.

The prior art inventions permit the private key to be held by other entities than the user, because of different security concerns. Mazzagatte is primarily concerned with protecting documents stored in the server. To that end, the printer accessing the server controls the private key. DeBry is primarily concerned with the security of the file source. To that end, the file source controls the private key. The Applicant is seeking to protect the person who is printing a document. To that end, the person printing controls the private key. Since the user does not control the private key, neither of the prior art processes is as secure as the Applicant's claimed process, as least from the point of view of the user.

Considered from the perspective of the second *prima facie* requirement, even if an expert were given the Mazzagatte and DeBry inventions as a foundation, there is no reasonable expectation that this expert could derive the claimed invention, since the claimed invention describes an invention where the user (the person printing a document) holds the private key. As noted above, the prior art references do not suggest that the person actually printing the document is the party in need of protection.

With respect to the third *prima facie* requirement, even if the references are combined, they do not disclose all the elements of the claimed invention. The Applicant's base claims recite encrypting a document with a public key, accepting a private key at the printer, and decrypting the document with the private key. Mazzagatte does not describe the transmission of a document using a public/private key pair.

DeBry does not encrypt a document using a public key, but rather, encrypts a symmetric key using a public key. Likewise, DeBry does not decrypt a document using a private key, but rather, uses a private key to recover the symmetric key.

In summary, neither of the prior art references describes a process that encrypts a document with a public key at the source, or decrypts the document at the destination printer using a private key. As mentioned above, the practical result of the Applicant's limitations is an added security enjoyed by neither of the references. Only the claimed invention limitations prevent a document from printing, until the user arrives at the printer and submits their private key.

The combination of Mazzagatte with DeBry does not explicitly describe all the limitations of claims 1, 12, 19, and 29. Neither do the references suggest any modifications that that make the Applicant's independent claims obvious. Claims 2-8 and 10-11, dependent from claim 1, claims 13-18, dependent from claim 12, claims 20-25 and 27-28, dependent from claim 19, and claims 30-35, dependent from claim 29, enjoy the same distinctions from the cited prior art.

SUMMARY AND CONCLUSION

It is submitted that for the reasons pointed out above, the claims in the present application clearly and patentably distinguish over the cited references. Accordingly, the Examiner should be reversed and ordered to pass the case to issue.

A check is enclosed, in the amount of $500.00, to cover the fee for this Appeal Brief. Authorization is given to charge any deficit or credit any excess to Deposit Account No. 502033.

Respectfully submitted,

Date: 10/1/2005

Gerald Maliszewski
Registration No. 38,054

Customer Number 55,286
P.O. Box 270829
San Diego, CA 92198-2829
Telephone: (858) 451-9950
Facsimile: (858) 451-9869
gerry@ipatentit.net

TABLE OF CONTENTS

CLAIMS APPENDIX

1. (previously presented) In a network of connected devices, a communications security method comprising:

encrypting documents with a public key;

spooling the encrypted documents to a network-connected file server;

notifying the printer of encrypted documents spooled on the network file server;

at the printer, accepting a private key corresponding to the public key used to encrypt the documents;

following the acceptance of the private key, transmitting the encrypted documents to a network-connected printer;

decrypting the documents with the private key; and,

printing the decrypted documents.

2. (previously presented) The method of claim 1 wherein encrypting the documents with a public key includes encrypting the documents at a network-connected computer having a public key encryption application; and,

wherein transmitting the encrypted documents to a network-connected printer includes transmitting the encrypted documents between the computer, file server, and the printer, through a network.

3. (original) The method of claim 2 wherein decrypting the documents with the private key includes operating the printer in response to the printer driver encryption software; and

the method further comprising:

supplying the printer driver encryption software to the computer.

4. (original) The method of claim 3 wherein supplying the printer driver encryption software to the computer includes:

supplying an application to optionally encrypt documents;

in response to the application, creating a graphical user interface (GUI) dialog box to invoke the document encryption option; and,

in response to invoking the document encryption option, creating a graphical user interface (GUI) dialog box to request and accept public key information.

5. (original) The method of claim 2 further comprising:

generating a plurality of public keys with corresponding private keys;

distributing the public keys universally to network-connected computers; and,

selectively distributing the private keys.

6. (original) The method of claim 5 in which the printer has a card reader to read code from SMART cards;

wherein selectively distributing the private keys includes distributing the private keys as SMART cards; and,

wherein accepting a private key includes using the code read by the printer card reader.

7. (original) The method of claim 5 in which the printer has a keyboard interface to accept an alpha-numeric code, and the method further comprising:

storing the private keys in the printer;

wherein selectively distributing the private keys includes:

selectively distributing alpha-numeric codes;

creating a table in the printer to cross-reference private keys with alpha-numeric codes; and,

wherein accepting the private keys includes using the private key referenced by the entered alpha-numeric code.

8. (previously presented) The method of claim 2 further comprising:

spooling the encrypted documents from the file server to a printer memory; and,

wherein decrypting the documents with the private key includes retrieving the encrypted documents from printer memory.

9. canceled

10. (original) The method of claim 2 further comprising:

in response to accepting the private key, generating a list of documents encrypted with the corresponding public key;

creating a graphical user interface (GUI) dialog box to invoke the selection of an encrypted document; and, wherein printing the documents includes printing the documents in response to selecting a document.

11. (original) The method of claim 1 wherein transmitting the encrypted documents to a network-connected printer includes transmitting a facsimile (FAX) transmission; and,

wherein decrypting the documents with the private key includes decrypting the encrypted FAX transmission.

12. (previously presented) A method for secure communications to a network-connected printer, the method comprising:

receiving documents spooled from a file server, encrypted with a public key;

accepting a private key corresponding to the public key used to encrypt the documents;

decrypting the documents with the private key; and,

printing the decrypted documents.

13. (original) The method of claim 12 wherein decrypting the documents with the private key includes operating the printer in response to publicly distributed printer driver encryption software.

14. (original) The method of claim 12 in which the printer has a card reader to read code from SMART cards; and,

wherein accepting a private key includes using the code read by the printer card reader as the private key.

15. (original) The method of claim 12 in which the printer has a keyboard interface to accept an alpha-numeric code, and the method further comprising:

storing the private keys in the printer;

creating a table in the printer to cross-reference private keys with alpha-numeric codes; and,

wherein accepting the private keys includes using the private key referenced by the entered alpha-numeric code as the private key.

16. (previously presented) The method of claim 12 further comprising:

spooling the encrypted documents from the file server into a printer memory; and,

wherein decrypting the documents with the private key includes retrieving the encrypted documents from printer memory.

17. (original) The method of claim 12 further comprising:

in response to accepting the private key, generating a list of documents encrypted with a corresponding public key;

creating a graphical user interface (GUI) dialog box to invoke the selection of an encrypted document; and,

wherein printing the documents includes printing the documents in response to selecting a document.

18. (original) The method of claim 12 wherein receiving documents encrypted with a public key includes receiving encrypted documents transmitted as a facsimile (FAX) transmission; and,

wherein decrypting the documents with the private key includes decrypting the encrypted FAX transmission.

19. (previously presented) A communications security system in a network of connected devices, the system comprising:

a computer having a network connection, an input to accept a public key, and an encryption application to supply encrypted documents to the network connection in response to accepting a public key;

a network connected to the computer to receive and transmit encrypted documents;

a file server connected to the network to receive encrypted documents from the computer; and,

a printer having an input connected to the network to accept encrypted documents from the file server, the printer having an input to accept a private key corresponding to the public key used to encrypt the documents at the computer, the printer having a decryption application to decrypt the documents with the private key, and the printer having an output to supply a printout of the decrypted documents.

20. (original) The system of claim 19 wherein the computer includes printer driver encryption software to generate the encryption application; and

wherein the printer is operated in response to the printer driver encryptions software loaded in the computer.

21. (original) The system of claim 20 wherein the computer has a display with an input connected to the application, wherein encryption application creates a graphical user interface (GUI) dialog box on the display to optionally invoke the encryption of documents, and in response to invoking the document encryption option, creates a GUI dialog box to request and accept public key information.

22. (original) The system of claim 19 further comprising:

a system administrator to generate a plurality of public keys with corresponding private keys, the system administrator distributing the public keys universally to network-connected computers, and selectively distributing the private keys.

23. (previously presented) The system of claim 22 further comprising:

private keys configured as code in SMART cards; and,

wherein the printer private key input is a card reader to read SMART cards, the printer using the code read by the card reader as the private key.

24. (original) The system of claim 22 wherein the system administrator generates a table cross-referencing the private keys to alpha-numeric codes, and selectively distributes the alpha-numeric codes; and,

wherein the printer private key input is a keyboard interface to accept private keys referenced by the alpha-numeric code entered on the keyboard, and the printer further comprising a memory to store the private keys, and a table to cross-reference private keys to alpha-numeric codes.

25. (previously presented) The system of claim 19 wherein the printer includes a memory to spool the encrypted documents received from the file server, the printer decrypting the documents with the private key by retrieving the encrypted documents from printer memory.

26. canceled

27. (original) The system of claim 19 wherein the printer has display connected to the decryption application to depict a list of documents encrypted with a corresponding public key, in response to accepting the private key;

wherein the printer decryption application creates a GUI dialog box on the display to invoke the selection of encrypted documents, the printer printing the documents in response to selecting a document from the GUI dialog box.

28. (original) The system of claim 19 wherein the computer transmits the encrypted documents as a facsimile (FAX) transmission;

wherein the network is a telephone system; and, wherein the printer decrypts the encrypted FAX transmission.

29. (previously presented) A secure communications network-connected printer, the printer comprising:

a network connection to receive documents from a file server, encrypted with a public key;

an input to accept a private key corresponding to the public key used to encrypt the documents;

an decryption application to decrypt the documents with the private key; and,

an output to supply a printout of the decrypted documents.

30. (original) The printer of claim 29 wherein the decryption application is responsive to publicly distributed printer driver encryption software.

31. (original) The printer of claim 29 wherein the private key input is a card reader to read code from SMART cards.

32. (original) The printer of claim 29 wherein the private key input is a keyboard interface to accept an alpha-numeric code; and,

the printer further comprising:

a memory to store the private keys;

a memory to store a table cross-referencing private keys with alpha-numeric codes; and, wherein private key input uses the private key referenced by the alpha-numeric code entered at the printer keyboard.

33. (previously presented) The printer of claim 29 further comprising:

a memory to spool the encrypted documents received from the file server; and,

wherein decryption application retrieves the encrypted documents from printer memory for decryption.

34. (original) The printer of claim 29 further comprising:

a display having an input;

wherein the decryption application creates a graphical user interface (GUI) dialog box application on the display to invoke the selection of an encrypted document, the GUI generating a list of documents encrypted with a corresponding public key, in response to accepting the private key; and,

wherein the documents are decrypted and printed in response to the documents being selected from the GUI.

35. (original) The system of claim 29 wherein the network connection is a telephone connection and the encrypted documents are facsimile (FAX) transmissions; and,

wherein the printer decrypts the encrypted FAX transmission.

EVIDENCE APPENDIX

ATTACHMENT A

SYSTEM AND METHOD FOR SECURE COMMUNICATIONS WITH NETWORK PRINTERS

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention generally relates to multifunction printing devices and, more particularly, to a system and method for adding security to the communications with a network-connected printing device.

2. Description of the Related Art

When a user wants to print confidential information using a networked printer, that user must take precautions that no one else is around the printer when the job is sent. Then, the user must hurry over to collect the printout before someone else goes to the printer, or before the confidential job is mixed up with someone else's job. Even if the user is situated near the printer, security can be foiled if the printer jams, so that the printing is delayed. Worse, the network can be slow or fail, causing the printing to be delayed, or leaving the user unsure of when, or if the ordered job will actually print. The user's security can also be compromised if they accidentally send the job to the wrong printer.

In addition, the data that is being sent to the printer can easily be captured at other network-connected computers or workstations using commercially available software programs. The document "spy" need only be connected to the network with an electromagnetic "sniffing" device. Then, the spy can capture confidential documents that a user originates or sends to a specific network address.

Fig. 1 is a schematic block diagram of a user printing a document to non-secure printer (prior art). The user is unable to see a crowd of people at the printer, or is unable to foresee other jobs arriving simultaneously with their job. A spy is also shown intercepting documents being sent to the printer.

It would be advantageous if print jobs to network printers could be made more secure from an unintended audience.

It would be advantageous if only the intended recipient of a print job could retrieve the printout at the printer.

It would be advantageous if network communications from a network-connected computer, or to a network-connected printer could avoid being captured.

SUMMARY OF THE INVENTION

The present invention enables a user to print a job to a network printer using some known security features in a new context. The job remains spooled and encrypted at the printer until the user goes to the printer to trigger a hardcopy printout. The invention adds security to printing by encrypting the data, using the public key of the user, before the data is sent to the printer. Then, at the printer, the data is decrypted by reading the private key from the user's SMART identification card, using a smart card reader.

Accordingly, a method is provided for secure communications to a network-connected printer. The method comprises: receiving documents encrypted with a public key; spooling the encrypted documents into a printer memory; accepting a private key corresponding to the public key used to encrypt the documents; in response to accepting the private key, generating a list of documents encrypted with a corresponding public key; creating a graphical user interface (GUI) dialog box to invoke the selection of an encrypted document; decrypting the documents with the private key; and, printing the decrypted documents in response to selecting a document.

The printer has a card reader to read code from SMART cards, and accepting a private key includes using the code read by the card reader as the private key. Alternately, the printer has a keyboard interface to accept an alpha-numeric code. Then, the method further comprises: storing the private keys in the printer; creating a table in the printer to cross-reference private keys with alpha-numeric codes. Then, the private key referenced by the entered alpha-numeric code is used.

Further, the encrypted documents can be facsimile (FAX) transmissions, and the printer can be operated as a decrypting FAX machine. Additional details of the secure communication method and a secure communications printing device are presented below.

BRIEF DESCRIPTION OF THE DRAWING

Fig. 1 is a schematic block diagram of a user printing a document to non-secure printer (prior art).

Fig. 2 is a schematic block diagram of the present invention communications security system in a network of connected devices.

Fig. 3 is a schematic block diagram of the first computer of Fig. 2.

Fig. 4 is a schematic block diagram of the first printer of Fig. 2.

Fig. 5 is a flowchart illustrating the present invention method for secure communications in a network of connected devices.

Fig. 6 is a flowchart illustrating the present invention method for secure communications to a network-connected printer.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Fig. 2 is a schematic block diagram of the present invention communications security system in a network of connected devices. The system 200 comprises a first computer 202, a second computer 204, and an *n*th computer 206. Each of the computers 202-206 has a network connection on line 208. Line 208 represents a network, connected to the computers 202-206 to receive and transmit encrypted documents. There are a number of network types that can be used to connect computers and printers, for example, WAN or LAN networks. The present invention is not limited to any particular type of network. A first secure communications printer 210 and a *p*th secure communications printer 212 have inputs connected to the network 208 to accept encrypted documents.

A system administrator 214 generates a plurality of public keys with corresponding private keys. The system administrator distributes the public keys universally to network-connected computers, for example, via email, and selectively distributes the private keys. The system administrator can be situated in an organization's intranet, or as a third party connected via the Internet.

Fig. 3 is a schematic block diagram of the first computer 202 of Fig. 2. The first computer 202 is representative of the other computers (not shown in this figure). The computer 202 can also be referred to as a workstation terminal or user terminal. The first computer 202 has an input 300 to accept a public key. The first computer 202 includes an encryption application 302 to supply encrypted documents to the network connection 208, in response to accepting a public key. The computer includes printer driver encryption software 304 for generating the encryption application.. Conventionally, the driver software 304 is loaded onto the computer for the purpose of formatting the documents into a form acceptable to the destination printer. In this particular application, the driver software 304 enables to computer to communicate encrypted documents to a destination printer capable of decrypting the documents.

The computer 202 has a display 306 with an input connected to the encryption application 302. The encryption application 302 creates a graphical user interface (GUI) dialog box 308 on the display 306 to optionally invoke the encryption of documents. In response to invoking the document encryption option, the GUI dialog box 308 requests and accepts public key information. The public keys can be maintained at a third party website, for example, maintained on a intranet system drive, or they can be downloaded via email from the system administrator.

It should be understood that the word "document" as used herein has its conventional meaning in most contexts. However, a document can also be any type of information that can be printed out. It should also be understood that the present invention is not limited to any particular type of public/private keying system. There are several public/private key systems in existence, such as the pretty good protection (PGP) and Rivest-Shamir-Alderman (RSA) systems, that can be used to enable the present invention. Generally, the keys are generated as pairs. The public keys are publicly distributed. A first user seeking to send a confidential message to a second user encrypts the message with the second user's public key. Once received, the second user decrypts the encrypted message using their private key. Thus, each private key has a corresponding public key.

Fig. 4 is a schematic block diagram of the first printer 210 of Fig. 2. The first printer 210 is representative of the other printer (not shown). The printer 210 has an input 400 to accept a private key corresponding to the public key used to encrypt the documents at the computer. The printer 210 has a decryption application 402 to decrypt the documents with the private key, and an output 404 to supply a printout of the decrypted documents. The printer 210 is operated in response to the printer driver encryption software loaded in the computer (see Fig. 3).

In one aspect of the invention, the private keys are code configured in SMART cards. The system administrator distributes a SMART card, with the private key, to each user. As is well known, SMART cards include a microprocessor powered by the card reader, and have capacity to hold a relatively long (large number of bytes) lengths of code. Then, the printer key input 400 is a card reader to read SMART cards. The printer 210 uses the code read by the card reader 400 as the private key.

Alternately, the system administrator (see Fig. 2) generates a table cross-referencing the private keys to alpha-numeric codes, and selectively distributes the alpha-numeric codes. Then, the private key input 400 is a keyboard interface to accept an alpha-numeric code. The printer 210 has a memory 406 to store the private keys, and a table 408 to cross-reference private keys to alpha-numeric codes. The printer 210 accepts private keys referenced by the alpha-numeric code entered at the printer keyboard 400.

In some aspects of the invention, the printer 210 includes a memory 410 to spool the encrypted documents. The printer 210 decrypts the documents with the private key by retrieving the encrypted documents from printer memory 410.

Alternately, the system 200 further comprises a file server connected to the network to receive encrypted documents from the computer and to transmit encrypted documents to the printer. Returning briefly to Fig. 2, the file server could be enabled with the system administrator 214. In Fig. 4 the printer 210 decrypts documents with the private key after retrieving the encrypted documents from the file server on line 208.

In some aspects of the invention, the printer 210 has display 412 connected to the decryption application 402. In response to accepting a private key, the display depicts a list of documents encrypted with the corresponding public key. The decryption application 402 creates a GUI dialog box 414 on the display 412 to invoke the selection of encrypted documents. The printer prints the documents at output 404 in response to selecting a document from the GUI dialog box 414.

As defined herein, a printing device is a device that creates a hardcopy printout. The printing device may be a conventional printer, or a multifunctional printing (MFP) device that incorporates scanning and facsimile (FAX) functions. The printer can also be a single-function FAX device. Returning to Fig. 2, when the computer 202 transmits the encrypted documents as a facsimile (FAX) transmission, the network 208 is a telephone system, and the printer 210 decrypts the encrypted FAX transmission.

As mentioned above, in one application of the present invention, the printers have a SMART card reader installed. Users who want to use the security features of the printer are provided with a SMART card that holds their private key code. The system administrator typically generates the public and private keys for these users, and stores them in the email address book, or the printer itself can store this information. Alternately, a third party can issue and distribute the keys.

When a user desires print security, the encrypt option is enabled in the print settings dialog box provided by the print driver. The print driver then uses the user's public key from the stored location to encrypt the data (document) before sending it to the printer. The print engine (printer), when it sees that the job is encrypted, simply spools the data on to storage in the printer, or to a storage location such as a network drive or file server. The user walks up to the printer and inserts their SMART card in the slot on the printer. The printer identifies the user and displays a list of jobs for that user on the printer display panel. Using the touch screen capabilities of the printers display panel, or an equivalent GUI mechanism, the printing is started. The printer uses the private key from the card to decrypt the encrypted document.

Instead of using a SMART card to identify a user, alternate embodiments of the invention use a display panel on the printer as an input device for entering the password information about the user. For example, a user's PIN number. Then, the code can be cross-referenced to a private key stored in the printer.

Fig. 5 is a flowchart illustrating the present invention method for secure communications in a network of connected devices. Although the method (and the method depicted by Fig. 6 below) is depicted as a sequence of numbered steps for clarity, no order should be inferred from the numbering unless explicitly stated. The method starts at Step 500. Step 502 encrypts documents with a public key. Step 504 transmits the encrypted documents to a network-connected printer. Step 506, at the printer, accepts a private key corresponding to the public key used to encrypt the documents. Step 508 decrypts the documents with the private key. Step 510 prints the decrypted documents.

Encrypting the documents with a public key in Step 502 includes encrypting the documents at a network-connected computer having a public key encryption application. Then, transmitting the encrypted documents to a network-connected printer in Step 504 includes transmitting the encrypted documents from the computer, to the printer, through a network.

In some aspects of the invention a further step, Step 501, supplies printer driver encryption software to the computer. Decrypting the documents with the private key in Step 508 includes operating the printer in response to the printer driver encryption software. Supplying the printer driver encryption software to the computer in Step 501 includes substeps. Step 501 a supplies an application to optionally encrypt documents. Step 501b, in response to the application, creates a graphical user interface (GUI) dialog box to invoke the document encryption option. Step 501c, in response to invoking the document encryption option, creates a GUI dialog box to request and accept public key information.

Step 501d generates a plurality of public keys with corresponding private keys. Step 501e distributes the public keys universally to network-connected computers. In some aspects, the universe is limited to a defined users group or organization. Step 501f selectively distributes the private keys, generally one private key per user.

In some aspects of the invention, the printer has a card reader to read code from SMART cards. Then, selectively distributing the private keys in Step 501f includes distributing the private keys as SMART cards. Accepting a private key in Step 506 includes using the code read by the printer card reader.

Alternately, the printer has a keyboard interface to accept an alpha-numeric code, and the method comprises further steps. Step 501g stores the private keys in the printer, and selectively distributing the private keys in Step 501f includes substeps. Step 501f1 (not shown) selectively distributes alpha-numeric codes. Step 501f2 (not shown) creates a table in the printer to cross-reference private keys with alpha-numeric codes. Accepting the private keys in Step 506 includes using the private key referenced by the entered alpha-numeric code.

In some aspects, a further step, Step 505a, spools the encrypted documents in printer memory. Decrypting the documents with the private key in Step 508 includes retrieving the encrypted documents from printer memory. Alternately, Step 505a spools the encrypted documents to a network-connected file server. Step 501b notifies the printer of encrypted documents spooled on the network file server. Decrypting the documents with the private key in Step 508 includes the printer retrieving the encrypted documents from the file server.

Some aspects of the invention include further steps. Step 507a (not shown), in response to accepting the private key, generates a list of documents encrypted with the corresponding public key. Step 507b (not shown) creates a graphical user interface (GUI) dialog box to invoke the selection of an encrypted document. Then, printing the documents in Step 510 includes printing the documents in response to selecting a document in Step 507b.

In some aspects of the invention, transmitting the encrypted documents to a network-connected printer in Step 504 includes transmitting a facsimile (FAX) transmission. Then, decrypting the documents with the private key in Step 508 includes decrypting the encrypted FAX transmissions.

Fig. 6 is a flowchart illustrating the present invention method for secure communications to a network-connected printer. The method starts at Step 600. Step 602 receives documents encrypted with a public key. Step 604 accepts a private key corresponding to the public key used to encrypt the documents. Step 606 decrypts the documents with the private key. Decrypting the documents with the private key in Step 606 includes operating the printer in response to publicly distributed printer driver encryption software. Step 608 prints the decrypted documents.

In some aspects of the invention, the printer has a card reader to read code from SMART cards, and accepting a private key in Step 604 includes using the code read by the printer card reader as the private key. Alternately, the printer has a keyboard interface to accept an alpha-numeric code, and the method comprises further steps. Step 601a stores the private keys in the printer. Step 601b creates a table in the printer to cross-reference private keys with alpha-numeric codes. Then, accepting the private keys in Step 604 includes using the private key referenced by the entered alpha-numeric code as the private key.

In some aspects, a further step, Step 603 spools the encrypted documents into a printer memory, and decrypting the documents with the private key in Step 606 includes retrieving the encrypted documents from printer memory.

In some aspects of the invention, Step 605a, in response to accepting the private key, generates a list of documents encrypted with a corresponding public key. Step 605b creates a graphical user interface (GUI) dialog box to invoke the selection of an encrypted document. Printing the documents in Step 608 includes printing the documents in response to selecting a document.

When receiving documents encrypted with a public key (Step 602) includes receiving encrypted documents transmitted as a facsimile (FAX) transmission, then decrypting the document with a private key in Step 606 includes decrypting the encrypted FAX transmissions.

A system and method have been provided for making communications secure to a network-connected printer. Examples have been given of protecting printing and FAX transmission jobs, however, the present invention is not limited to just these applications. Public/private key sets have been described as the security means. However, other variations and embodiments of the invention will occur to those skilled in the art.

WE CLAIM:

ATTACHMENT B

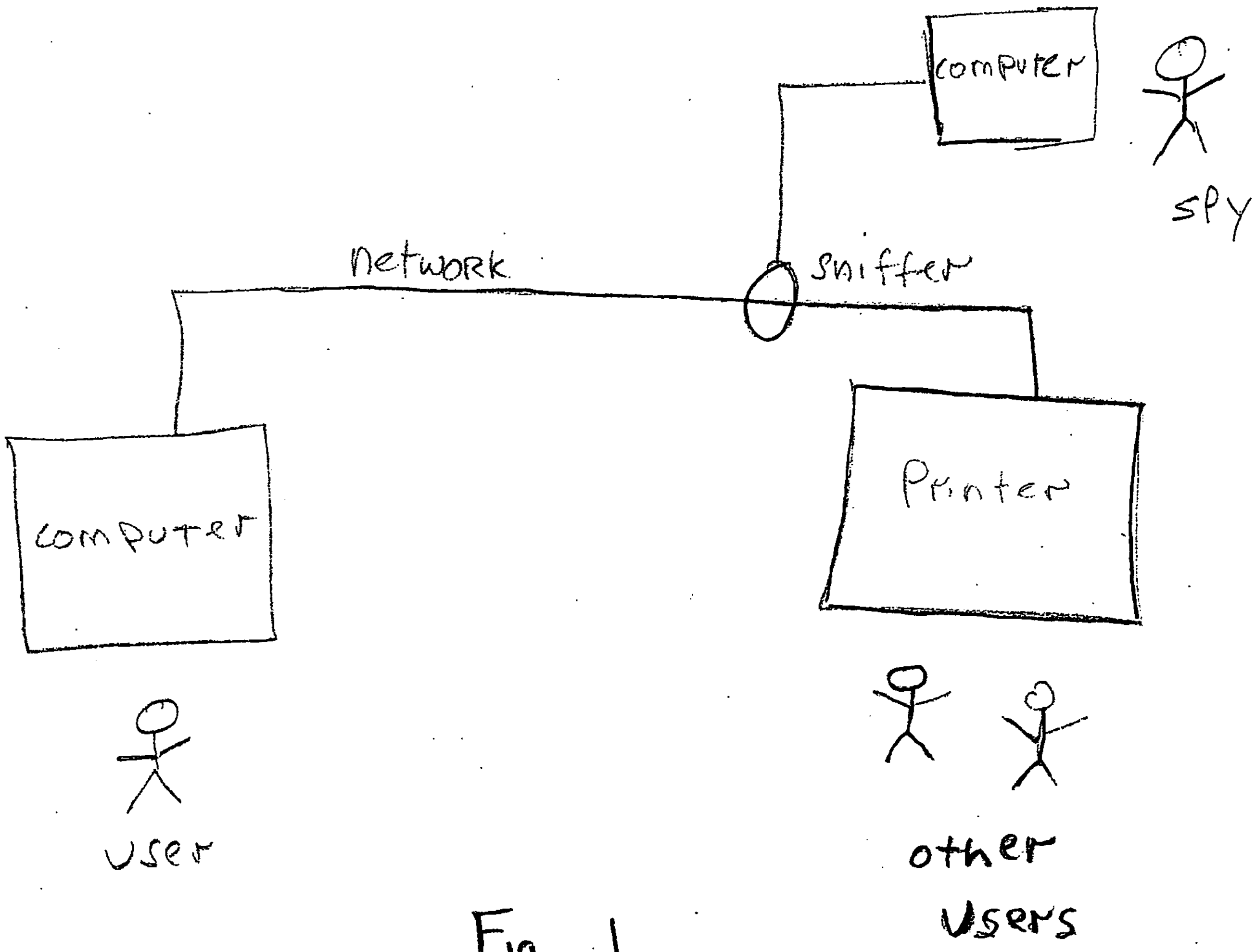


Fig. 1
(Prior art)

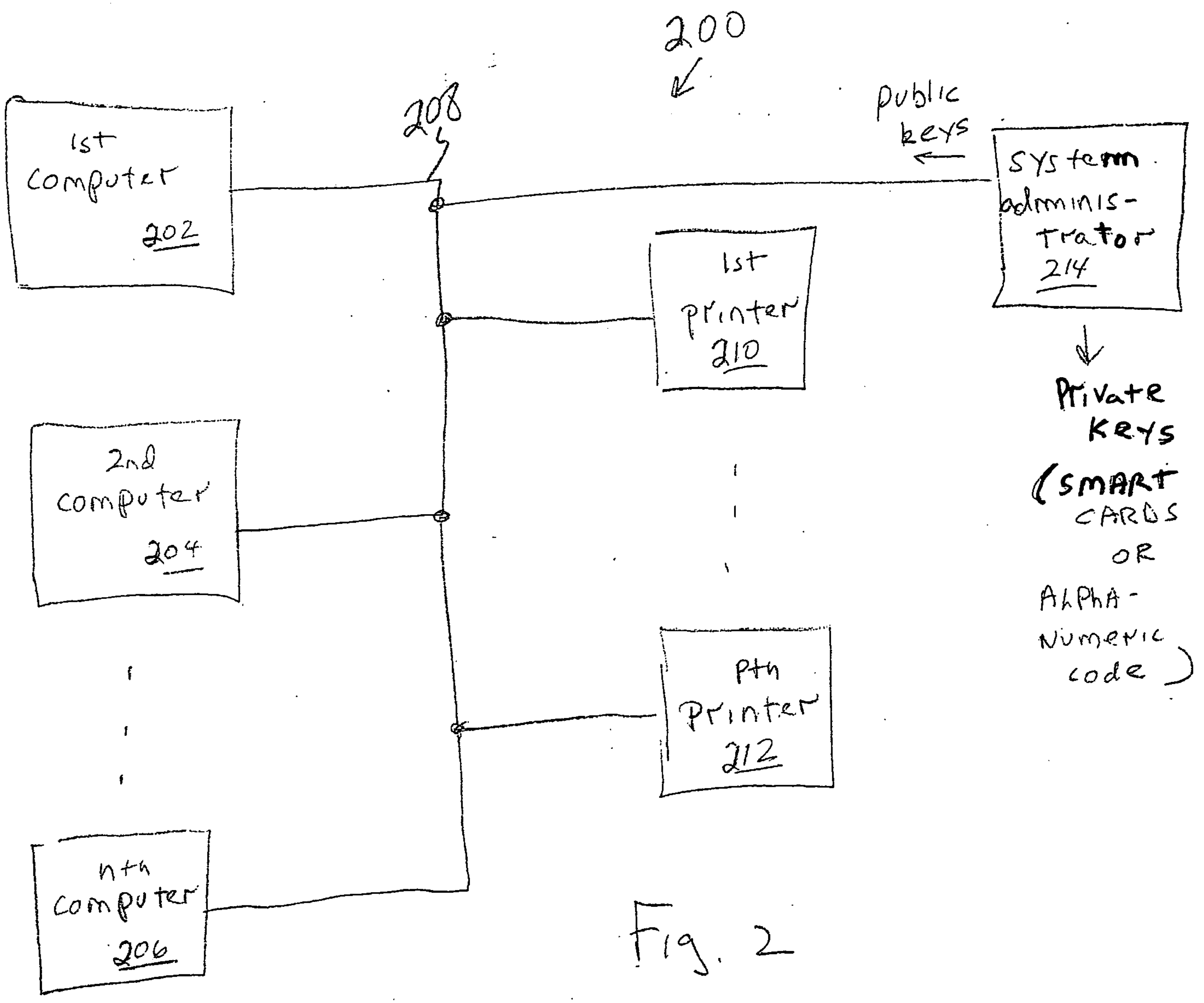

200
208
1st computer 202
2nd computer 204
nth computer 206
1st printer 210
Pth printer 212
public keys
System adminis-trator 214
Private Keys (SMART CARDS OR AlPhA-Numeric code)

Fig. 2

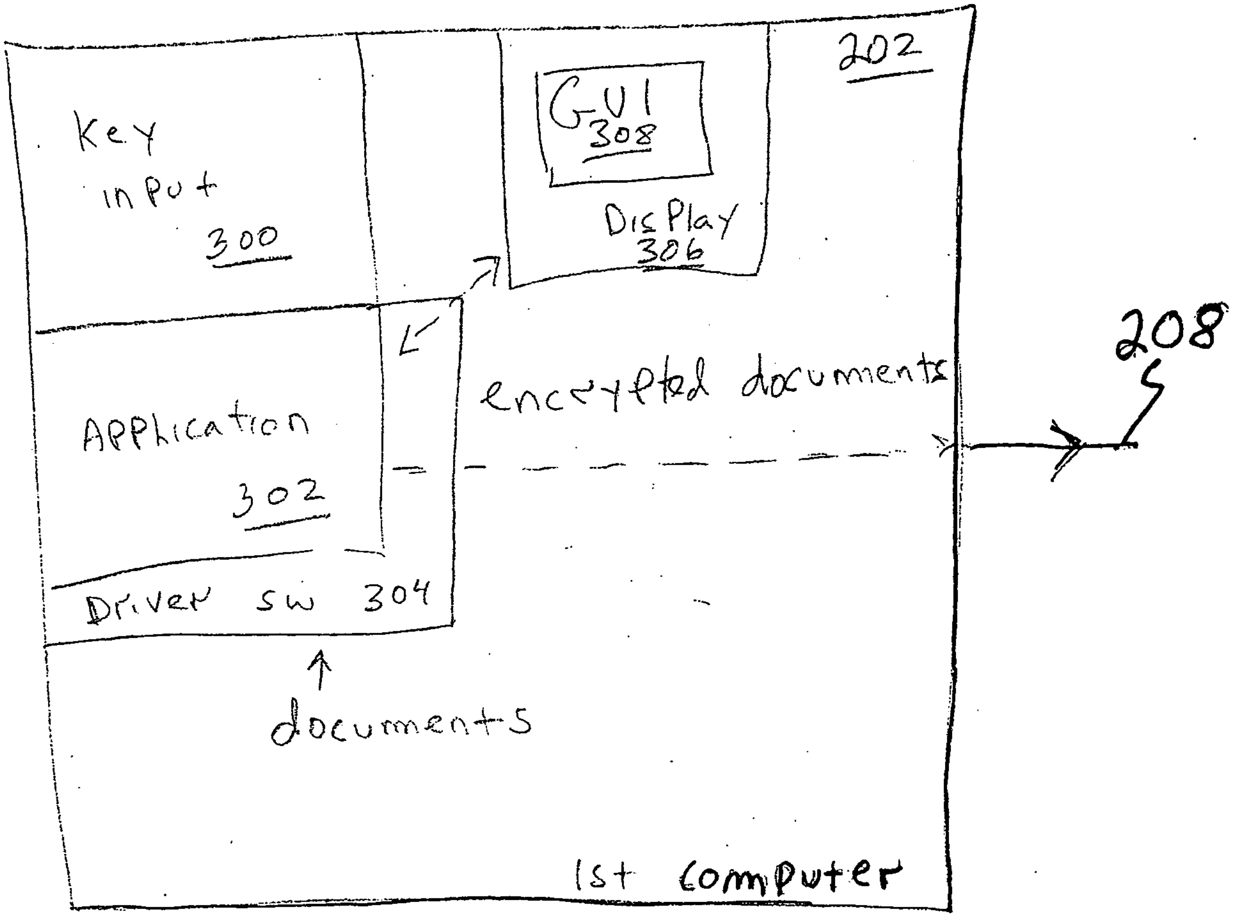

202
Key input 300
GUI 308
Display 306
Application 302
Driver sw 304
encrypted documents
208
documents
1st computer

Fig. 3

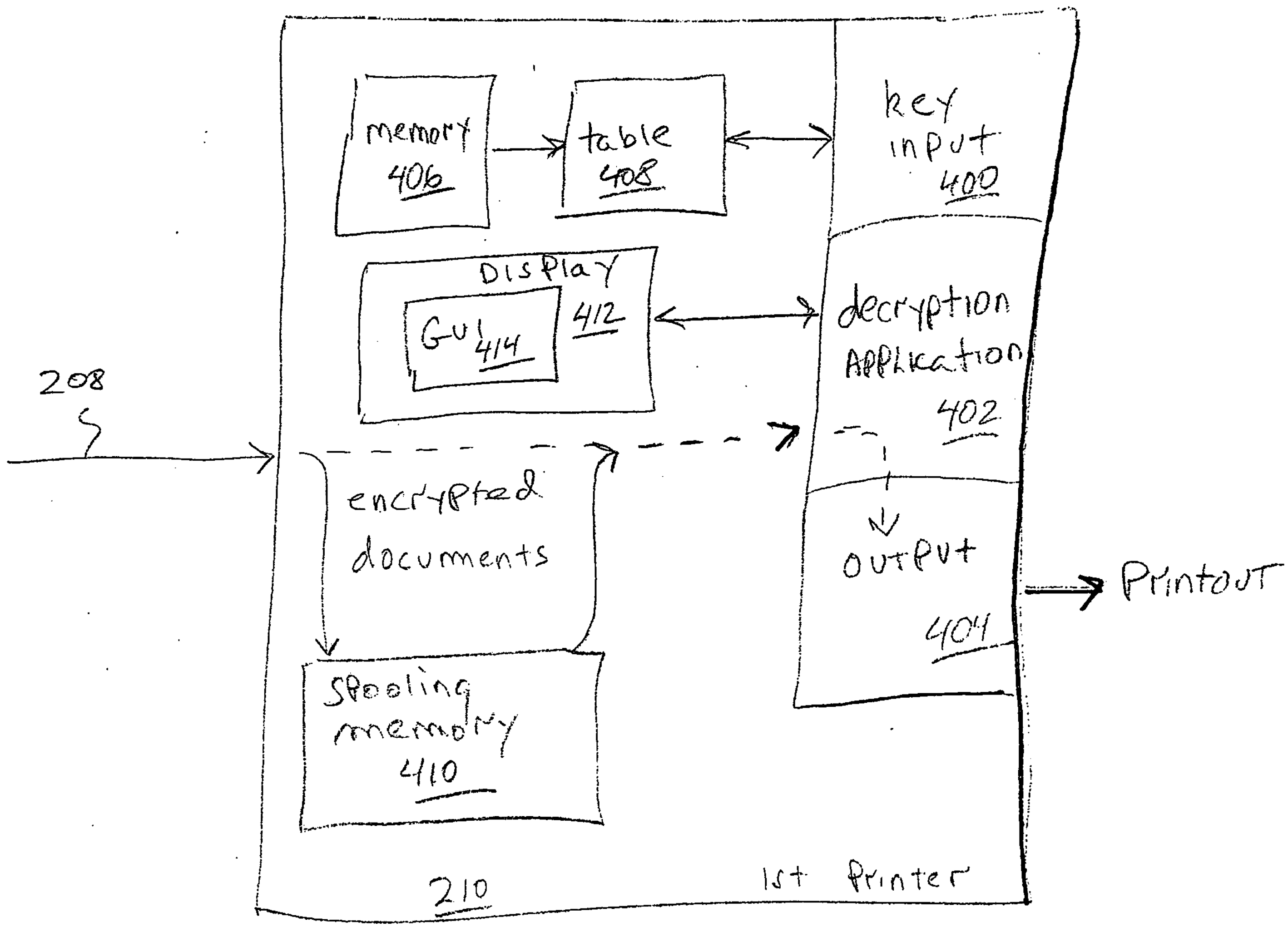
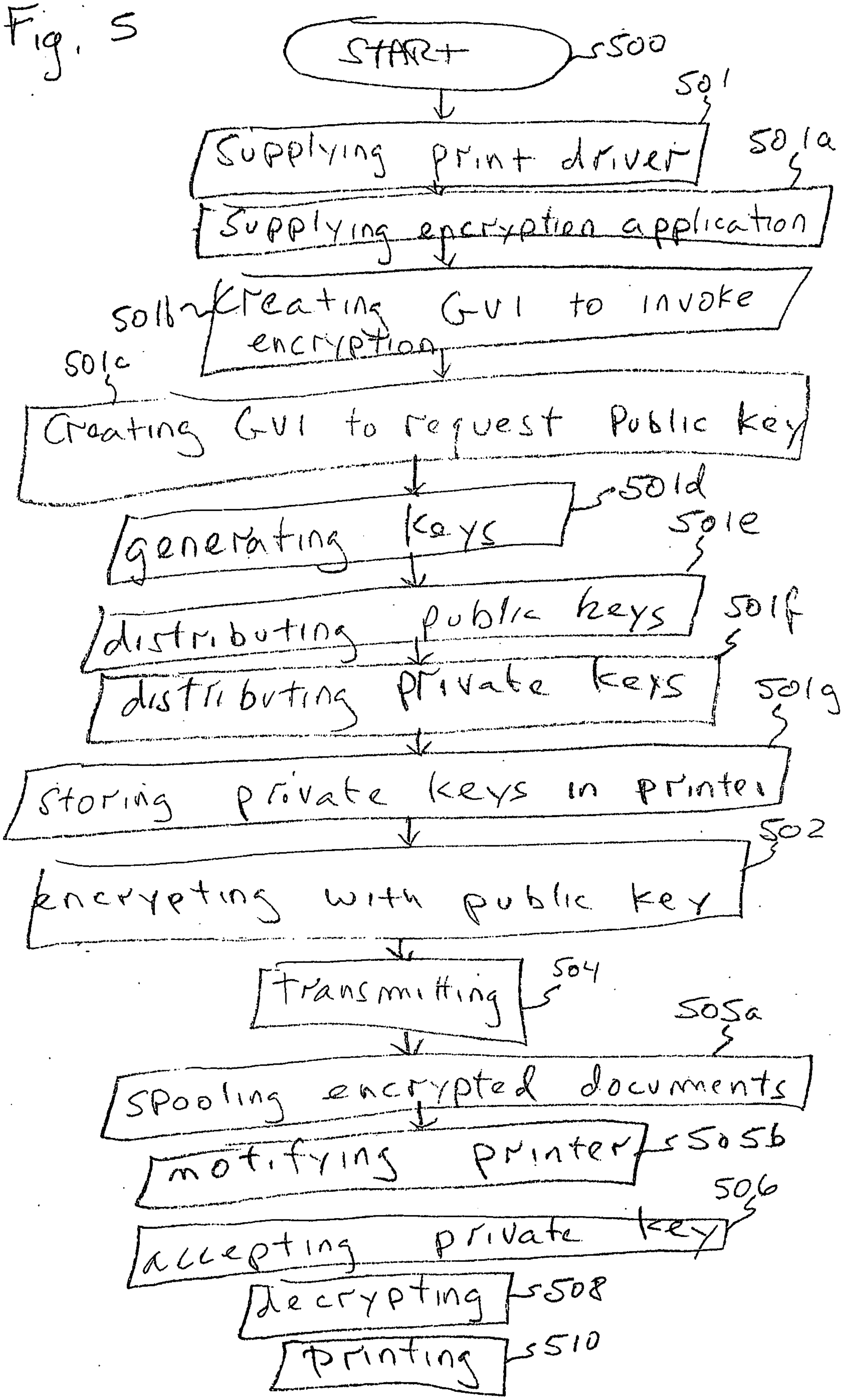

memory
406
table
408
key
input
400
Display
GUI
414
412
decryption
Application
402
208
encrypted
documents
output
404
Printout
Spooling
memory
410
210
1st Printer

Fig. 4

Fig. 5


START
500
501
Supplying print driver
501a
Supplying encryption application
501b
Creating GUI to invoke encryption
501c
Creating GUI to request Public key
501d
generating keys
501e
distributing public keys
501f
distributing private keys
501g
storing private keys in printer
502
encrypting with public key
504
Transmitting
505a
spooling encrypted documents
505b
motifying printer
506
accepting private key
508
decrypting
510
printing

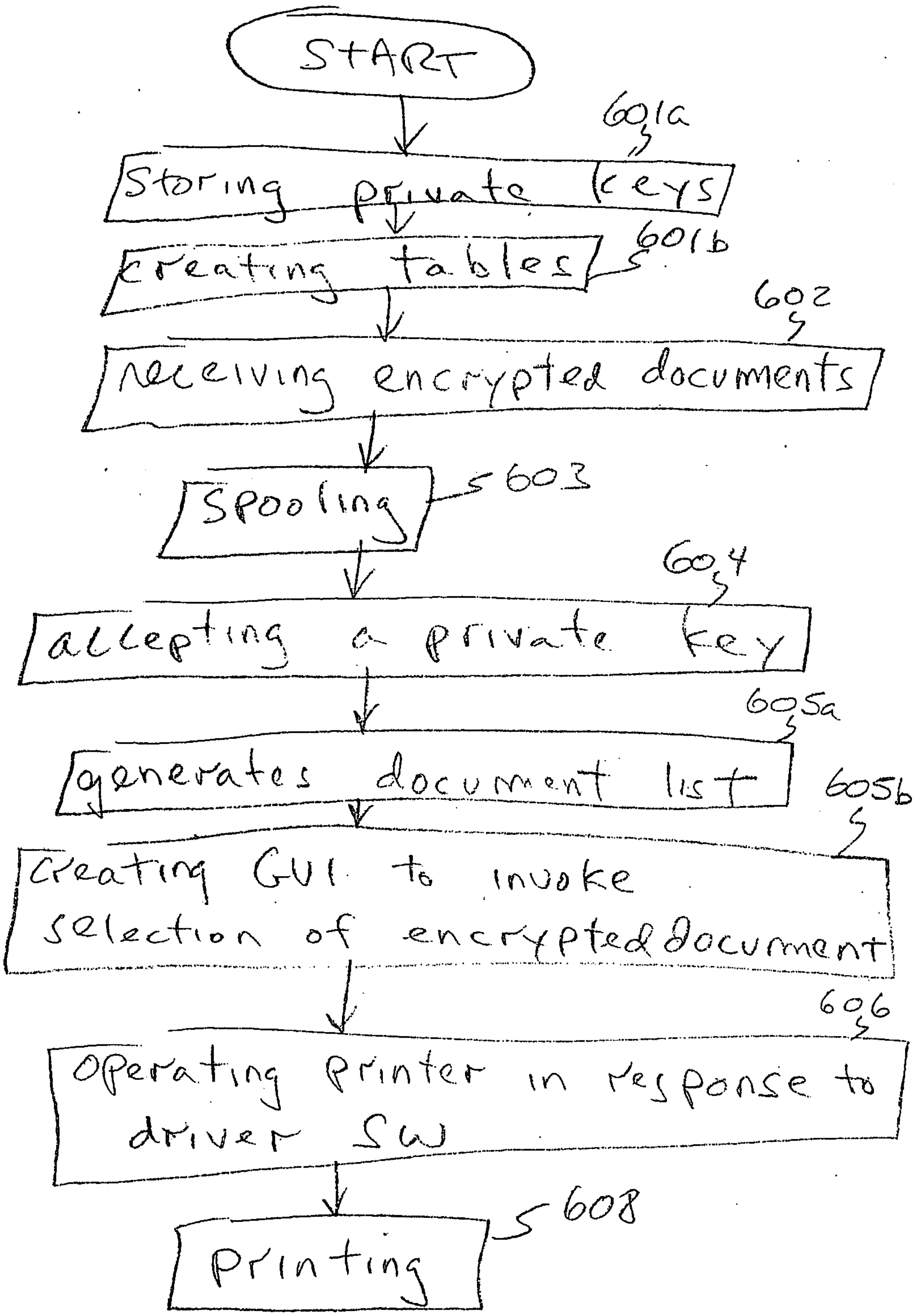

START
601a
Storing private keys
601b
creating tables
602
receiving encrypted documents
603
Spooling
604
accepting a private key
605a
generates document list
605b
Creating GUI to invoke selection of encrypted document
606
Operating printer in response to driver SW
608
Printing

Fig. 6

ATTACHMENT C

US006862583B1

(12) **United States Patent**
Mazzagatte et al.

(10) **Patent No.: US 6,862,583 B1**
(45) **Date of Patent: Mar. 1, 2005**

(54) **AUTHENTICATED SECURE PRINTING**

(75) Inventors: **Craig Mazzagatte**, Aliso Viejo, CA (US); **Royce E. Slick**, Mission Viejo, CA (US); **Neil Iwamoto**, Mission Viejo, CA (US)

(73) Assignee: **Canon Kabushiki Kaisha**, Tokyo (JP)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/411,665**

(22) Filed: **Oct. 4, 1999**

(51) **Int. Cl.**^{7} **H04L 9/32**; G06F 1/24

(52) **U.S. Cl.** **705/64**; 380/25; 380/51; 380/55; 705/51; 705/57; 713/155

(58) **Field of Search** 380/18, 21, 25, 380/51; 705/51, 57

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,191,611	A	*	3/1993	Lang	380/25
5,392,351	A		2/1995	Hasebe et al.	380/4
5,398,283	A	*	3/1995	Virga	380/18
5,495,533	A	*	2/1996	Linehan et al.	380/21
5,606,613	A	*	2/1997	Lee et al.	380/21
5,633,932	A	*	5/1997	Davis et al.	380/25
5,720,012	A		2/1998	McVeigh et al.	395/113
5,752,697	A		5/1998	Mandel et al.	271/288
5,903,646	A		5/1999	Rackman	380/4
5,933,498	A		8/1999	Schneck et al.	380/4
5,933,501	A		8/1999	Leppek	380/21
5,949,881	A		9/1999	Davis	380/25
6,111,953	A	*	8/2000	Walker et al.	380/51
6,314,521	B1		11/2001	Debry	713/201
6,343,361	B1		1/2002	Nendell et al.	713/171
6,378,070	B1		4/2002	Chan et al.	713/155
6,385,728	B1		5/2002	DeBry	713/201
6,430,690	B1		8/2002	Vanstone et al.	713/182
6,466,921	B1		10/2002	Cordery et al.	705/60

FOREIGN PATENT DOCUMENTS

EP	0 542 703	5/1993	
EP	0 657 845	6/1995	
EP	0 671 830	9/1995	
EP	0 858 021	8/1998	
EP	0 935 182	8/1999	
EP	0 935 182 A1 *	8/1999	G06F/1/00
JP	3-269756	2/1991	
WO	WO 98/07254	2/1998	

OTHER PUBLICATIONS

Dannenberg, Roger B., et al., "A Butler Process for Resource Sharing on Spice Machines", ACM Transactions on Office Information Systems, vol. 3, No. 3, pp. 234–252, Jul. 1985.

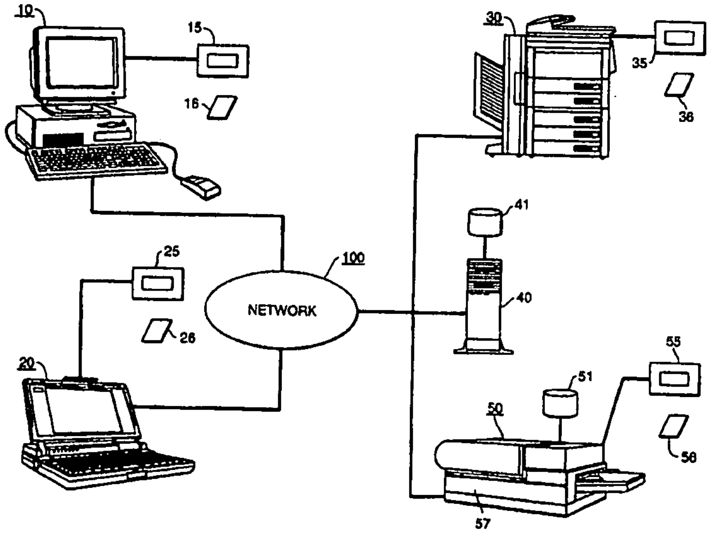
* cited by examiner

Primary Examiner—John W. Hayes
Assistant Examiner—Daniel L. Greene
(74) *Attorney, Agent, or Firm*—Fitzpatrick, Cella, Harper & Scinto

(57) **ABSTRACT**

Authorized printout of an image corresponding to print data received at a print node from a network. The authorized printout comprises encrypting print data by a print node and storing the encrypted print data without printout, receiving authentication of an intended recipient to print the print data, and decrypting the encrypted print data by the print node and printing the decrypted print data by an image forming device, responsive to receipt of authentication in the receiving step. The print node may be the image forming device itself or a gateway to multiple image forming devices. The print node encrypts the print data with either a symmetric key or an asymmetric key.

50 Claims, 9 Drawing Sheets



ATTACHMENT D

US006385728B1

(12) United States Patent
DeBry

(10) Patent No.: US 6,385,728 B1
(45) Date of Patent: May 7, 2002

(54) SYSTEM, METHOD, AND PROGRAM FOR PROVIDING WILL-CALL CERTIFICATES FOR GUARANTEEING AUTHORIZATION FOR A PRINTER TO RETRIEVE A FILE DIRECTLY FROM A FILE SERVER UPON REQUEST FROM A CLIENT IN A NETWORK COMPUTER SYSTEM ENVIRONMENT

(75) Inventor: Roger K. DeBry, Longmont, CO (US)

(73) Assignee: International Business Machines Corporation, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: 08/978,793

(22) Filed: Nov. 26, 1997

(51) Int. Cl.^{7} G06F 11/00
(52) U.S. Cl. 713/201; 709/229; 713/200
(58) Field of Search 380/25, 49; 709/229; 713/201, 202; 707/1, 9; 340/825.34

(56) References Cited

U.S. PATENT DOCUMENTS

5,005,200	A		4/1991	Fischer	380/30
5,014,221	A		5/1991	Mogul	364/519
5,214,702	A		5/1993	Fischer	380/30
5,473,691	A		12/1995	Menezes et al.	380/25
5,537,626	A		7/1996	Kraslavsky et al.	395/828
5,544,322	A		8/1996	Cheng et al.	395/200.12
5,633,932	A	*	5/1997	Davis et al.	713/176
5,742,759	A	*	4/1998	Nessett et al.	713/201

FOREIGN PATENT DOCUMENTS

JP	08-212293	8/1996
TW	273061	3/1996
WO	WO96/25812	8/1996

OTHER PUBLICATIONS

G. Walter, "Packetprint for Electronic Signature or Message Authentication", IBM Technical Disclosure Bulletin, vol. 23, No. 7B, pp. 3325–3327, Dec. 1980.

D.E. Coe et al., "Developing and Deploying a Corporate Wide Digital Signature Capability", SIGSAC Rev. (USA), vol. 13, No. 3, pp. 5–8, Jul. 1995.

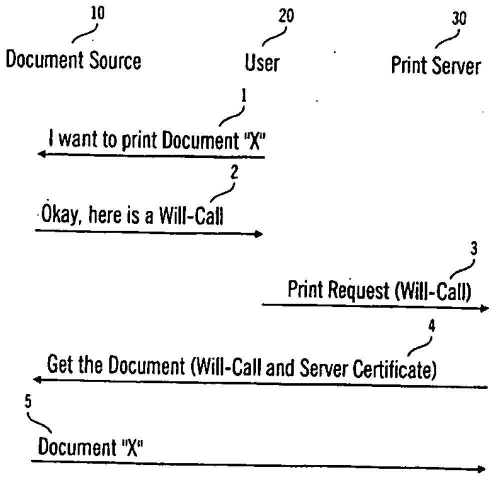
* cited by examiner

Primary Examiner—Gail Hayes
Assistant Examiner—Ho S. Song
(74) *Attorney, Agent, or Firm*—David W. Victor; Konrad Raynes Victor & Mann

(57) ABSTRACT

The system, method, and program of this invention enables a client system to pass authorization, received from a file source, to a printer to retrieve and print a file directly from the file source without the client system ever receiving a copy of the file. The client system, print server, and file source are communicatively connected across a network. When the client system requests authorization from the file source, the file source creates a "will-call" certificate which contains the distinguished name of the file source, a path to the file, a digital signature of the file source, a validity date, and a unique tracking number for that certificate created by that file source. The will-call certificate is sent to the client, which sends it on to the print server. The print server uses the distinguished name of the file source and path to the file in the will-call certificate to locate the file and request the file directly from the file source. The print server's request to the file source also includes the will-call certificate. The file source can verify various aspects of the will-call certificate's validity through the digital signature, the validity date, and/or the tracking number. If the request is valid, the file source sends the file directly to the print server.

51 Claims, 5 Drawing Sheets


10
Document Source
20
User
30
Print Server
1
I want to print Document "X"
2
Okay, here is a Will-Call
3
Print Request (Will-Call)
4
Get the Document (Will-Call and Server Certificate)
5
Document "X"